

IN THE CLAIMS:

1 Claims 1-11 (Canceled)

1 12. (Currently Amended) A method for limiting the operational life of software in a
2 network environment, the method comprising:

3 providing a program applet embedded with an associated password
4 to a client via a network;

5 receiving from said program applet via said network a request for
6 information stored in a restricted access storage area[.];

7 further receiving from said program applet said [request comprising
8 said] associated password, for authentication;

9 authenticating said associated password;

10 thereafter providing said information to said program applet via said
11 network while said associated password is valid; and

12 invalidating said password coincident with an invalidation event.

1 13. (Currently amended) A method according to claim 12 wherein said invalidating
2 comprises invalidating said associated password at a predetermined time.

1 14. (Currently amended) A method according to claim 12 wherein said invalidating
2 comprises invalidating said associated password after a predetermined elapsed time
3 from when said request was received.

1 15. (Currently amended) A method according to claim 12 wherein said invalidating
2 comprises invalidating said associated password upon the detection of a loss of
3 communication with said client.

1 16. (Cancelled)

1 17. (Cancelled)

1 18. (Currently amended) A method according to claim 12 wherein said providing
2 comprises generating said associated password at a server upon receiving said
3 request at said server.

1 Claims 19-26 (Canceled)

1 27. (Currently Amended) A network-based software authentication system
2 comprising a server, the server comprising:

- 3 a password generator;
4 password validation apparatus;
5 a restricted-access storage area;
6 a program applet; and
7 invalidation apparatus;

8 wherein said server is operative to:

- 9 a) cause said password generator to generate a password;
10 b) embed said password within said program applet, and provide
11 said program applet embedded with said password to a client via a network;
12 c) receive a request for information and receive said password, for
13 authentication, from said program applet via said network[, said request comprising
14 said associated password];
15 d) authenticate said password using said password validation
16 apparatus;
17 e) provide said information to said program applet via said network
18 while said associated password is valid; and
19 f) invalidate said password using said invalidation apparatus
20 coincident with an invalidation event.

1 28. (Original) A system according to claim 27 wherein said invalidation event
2 comprises the arrival of a predetermined time.

1 29. (Original) A system according to claim 27 wherein said invalidation event
2 comprises the elapsing of a predetermined elapsed time from when said request was
3 received.

D 1 30. (Original) A system according to claim 27 wherein said invalidation event
2 comprises the detection of a loss of communication with said client.

1 31. (Cancelled)

1 32. (Cancelled)

1 33. (Original) A system according to claim 27 wherein said password is generated at
2 said server upon receiving said request at said server.
